PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	Ober, et al.	Examiner:	Unassigned
Serial No.:	Unassigned	Group Art Unit:	Unassigned
Confirmation No.:	Unassigned	Docket:	621-31 CON
Filed:	Herewith	Dated:	July 2, 2001
For:	CRYPTOGRAPHIC KEY MANAGEMENT SCHEME		

Commissioner for Patents
Washington, DC 20231

I hereby certify this correspondence is being deposited with the United States Postal Service as Express Mail No: EL470331190US, postpaid in an envelope, addressed to:
Commissioner for Patents, Washington, D.C. 20231 on *July 2, 2001*

Signature: Joyce Peterson

PRELIMINARY AMENDMENT

Sir:

Prior to examination of the above-identified application on the merits, please amend the application as follows:

IN THE SPECIFICATION:

On page 1, replace the paragraph beginning at line 2 with the following:

This application is a continuation of Application Serial No. 09/154,133, filed on September 16, 1998 and is based on Provisional Patent Application Serial Nos. 60/059,082 and 60/059,839, each of which was filed on September 16, 1997, and relates to U.S. Patent Application Serial No. 09/154,443 filed on September 16, 1998, the disclosures of which are incorporated herein by reference.

IN THE CLAIMS:

Please cancel Claim 1 without prejudice.

Please add new Claim 2 as follows:

--2. A method of managing encryption keys in a cryptographic co-processor, which comprises the steps of:

selecting a key type from one of a symmetrical key type and an asymmetrical key type, wherein a user selects the key type;

selecting a bit length;

generating a key, the generated key having the selected key type and the selected bit length, the step of generating a key being performed in at least one way selected from a group of ways consisting of: 1) sampling an output of a random number generator to assemble a desired length data encryption key (DEK); 2) sampling an output of a random number generator to assemble a desired length key encryption key (KEK); 3) performing a Diffie-Hellman g^{xy} exponentiation in order to arrive at a shared secret value; 4) deriving a symmetrical secret key by hashing an application supplied password or passphrase; 5) transforming an existing key; and 6) importing an unencrypted (RED) key provided by the application; and

representing the generated key in one of an external form and an internal form, the method of managing encryption keys supporting an internally generated storage variable, a local storage variable and a user application generated KEK.--.

REMARKS

Original Claim 1 filed in the parent application Serial No. 09/154,133 has been cancelled without prejudice and new Claim 2 has been added. Specifically, Claim 2 incorporates Claim 1 following clarification that a key may be generated by transforming an existing key without specifying the transformation algorithm.

Accordingly, it is respectfully urged that new Claim 2 patentably distinguishes over the references cited in the parent application and is allowable.

In view of the following amendments and remarks, entry and favorable consideration of new Claim 2, and allowance of the application with Claim 2 are respectfully solicited.

Respectfully submitted,

Rod S. Turner
Registration No.: 38,639
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550
RST/jp

136769_1.DOC

VERSION OF AMENDMENT WITH MARKS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

On page 1, replace the paragraph beginning at line 2 with the following:

This application is a continuation of Application Serial No. 09/154,133, filed on September 16, 1998 and is based on Provisional Patent Application Serial Nos. 60/059,082 and 60/059,839, each of which was filed on September 16, 1997, and relates to U.S. [patent application entitled "Cryptographic Co-Processor"] Patent Application Serial No. 09/154,443 filed [concurrently herewith] on September 16, 1998, the disclosures of which are incorporated herein by reference.

IN THE CLAIMS:

Please cancel Claim 1 without prejudice.

Please add new Claim 2 as follows:

--2. A method of managing encryption keys in a cryptographic co-processor, which comprises the steps of:

selecting a key type from one of a symmetrical key type and an asymmetrical key type, wherein a user selects the key type;

selecting a bit length;

generating a key, the generated key having the selected key type and the selected bit length, the step of generating a key being performed in at least one way selected from a group of ways consisting of: 1) sampling an output of a random number generator to assemble a desired length data encryption key (DEK); 2) sampling an output of a random number generator to assemble a desired length key encryption key (KEK); 3) performing a Diffie-Hellman g^{xy} exponentiation in order to arrive at a shared secret value; 4) deriving a symmetrical secret key by hashing an application supplied password or passphrase; 5) transforming [a] an existing key [using at least one of hashing, mixing with fixed data and rehashing, and exclusive oring (XORing)]; and 6) importing an unencrypted (RED) key provided by the application; and

representing the generated key in one of an external form and an internal form, the method of managing encryption keys supporting an internally generated storage variable, a local storage variable and a user application generated KEK.--.